12.1 INTRODUCTION

(PTU 2011)

Security of data has become the most significant issue of modern computing. Data in the database needs to be protected against unauthorised access, accidental or intentional loss, misuse etc. The goal of database security is the protection of data against such threats. The DBA of an organisation must identify such threats and enforce various security measures to protect the data.

12.2 THREATS TO DATABASE SECURITY

Some threats of database security are given below:

1. **Loss of confidentiality.** If an unauthorised person is able to access critical data then secrecy of information get lost.
2. **Authentication.** Whenever someone wants to access data, firstly his identity should be verified. If an unauthorised person access the data, then he can misuse it.
3. **Loss of integrity.** Data present in the database may get corrupted and do not match with original or actual data.
4. **Non-repudiation.** Suppose some person modifies the data and later denies that he has done it.
5. **Loss of availability.** It means data cannot be accessed by a user due to unavailability of hardware, network or applications.
6. **Theft or fraud.** It may lead to loss of confidentiality or loss of privacy of data.
7. **Accidental losses.** May be caused due to hardware, software or human error.

12.3 DATABASE SECURITY MEASURES

(PTU 2009)

The DBMS must provide technique to ensure the security of data against the above discussed threat such as:

12.3.1 Authentication

It is a process by which identity of a user is checked, i.e. whether the person is the correct person to access the database. Mostly passwords are used for authentication. These passwords are assigned by DBMS.

12.3.2 Authorisation

It is a process of granting of right to a user to have access to a system or a database. It is used to determine which user can access which portion of the database.

Therefore authorisation are also sometimes called access control.

Example: A user can access the data for reading only but he cannot delete or modify that data. There are two types of access control:

(a) ***Discretionary control.*** Users of the database have been given some access rights or privileges to use some or all portion of the database.

Example: User 1 can access a table containing salary information of employee, but user 2 cannot.

(b) ***Mandatory control.*** Data in the database is classified according to some criteria such as secret, confidential, sensitive information i.e. the data has a classification level and each user of the database has a clearance level i.e. upto which level he can access the data.

Example: For following classification level
Secret = 1, Confidential = 2
The query generated by a user (whose clearance level class is 2)

Select Name, Salary from Employee
where salary > 50,000
would be automatically be converted to
Select Name, Salary from Employee
where Salary > 50,000 and class > = 2

So, the user 2 can only retrieve rows which have a clearance level of 2 or more.

(PTU 2011)

12.3.3 Privileges

It refers to granting of access right to a user to access a particular database object. Privileges can be classified into:

1. **System privileges.** Granting permission to connect to the database, permission to create table etc.
2. **Object privileges.** Granting permission to perform operation on a specific table such as:
   (i) inserting new rows to a table

(ii) updating information in the table
(iii) altering the table structure
(iv) access the data
(v) delete some or all rows of table
(vi) creating index of a table etc.

Granting of privileges. A user or DBA can grant his access rights to any other user.

Example: Suppose DBA wants to give privilege to Satish to perform an update operation on table employee. Then DBA will execute the following statement

"Grant update on employee to Satish".

After executing this statement the DBMS would check whether the user who executed this query has privilege to execute the grant command. If yes, then privilege is granted to Satish, otherwise the grant request is rejected.

➲ **Granting privileges to certain column only.**

User need to specify the column names to which privileges is granted.

"Grant update on employee (E_Id, Address) to Satish".

Now, Satish can only update column E_Id and Address but not other column of the table. DBA can also give privileges to a user to allow other to grant privilege. For this DBA execute the following query.

"Grant update on Employee to Amit with grant option";

Now, Amit can give only update privilege to other users on employee table.

***Example*: "Grant update on employee to Rajesh";**

***Taking away privileges*.** Revoke command can be used to take away the **privilege** granted to a user.

***Example*:** Revoke update on employee from Satish.

12.3.4 Roles

Many user of the database have some access rights. So, all these users can be grouped and authorisation can given to this particular group.

Disadvantage of this is that it would not be possible to find which operation is carried out by which user.